

Exhibit 6

1 WILLIAM L. ANTHONY (State Bar No. 106908)
2 ERIC L. WESENBERG (State Bar No. 139696)
3 MARK R. WEINSTEIN (State Bar No. 193043)
4 ORRICK, HERRINGTON & SUTCLIFFE, LLP
5 1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

6 STEVEN ALEXANDER (admitted *Pro Hac Vice*)
7 KRISTIN L. CLEVELAND (admitted *Pro Hac Vice*)
8 JAMES E. GERINGER (admitted *Pro Hac Vice*)
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391
Facsimile: (503) 228-9446

12 Attorneys for Defendant and Counterclaimant,
13 MICROSOFT CORPORATION

14 UNITED STATES DISTRICT COURT
15 NORTHERN DISTRICT OF CALIFORNIA
16 OAKLAND DIVISION

17 INTERTRUST TECHNOLOGIES
CORPORATION, a Delaware corporation,
18 Plaintiff,
19 v.
20 MICROSOFT CORPORATION, a
Washington corporation,
21 Defendant.

22 MICROSOFT CORPORATION, a
Washington corporation,
23 Counterclaimant,
24 v.

25 INTERTRUST TECHNOLOGIES
CORPORATION, a Delaware corporation,
26 Counter Claim-Defendant.

CASE NO. C01-1640 SBA

MICROSOFT CORPORATION'S
PATENT LOCAL RULE 4-1(a)
STATEMENT (LIMITED TO "MINI-
MARKMAN" CLAIMS)

28

1 Pursuant to Patent Local Rule 4-1(a), Microsoft submits below the claim terms, phrases,
2 and clauses of the twelve selected "Mini-Markman" patent claims that Microsoft presently
3 submits, subject to discussions with InterTrust, should be construed by the Court, in addition to
4 construing each claim as a whole.

5 Set forth in Section A, below, is a list of individual claim terms that Microsoft presently
6 submits, subject to discussions with InterTrust, should be construed by the Court. Individual
7 claim terms should be construed wherever they are found in these twelve claims.

8 Set forth in Section B, below, are the phrases and clauses that Microsoft presently
9 submits, subject to discussions with InterTrust, should be construed by the Court. The claim
10 phrases and clauses that Microsoft presently submits, subject to discussions with InterTrust,
11 should be governed by 35 U.S.C. § 112(6), are identified in Section B by double underlining.
12

13 Many of these claim terms, phrases and clauses are indefinite and otherwise improper
14 under 35 U.S.C. § 112(2), and Microsoft reserves all rights to assert those defects as to each of
15 these claim terms, phrases and clauses.

16 The grouping of individual claim terms below is for convenience only and does not imply
17 any particular connection, or lack of connection, between any terms.

18 **A. Individual Claim Terms**

- 21 • a digital file, digital file
- 22 • access, accessed, access to, accessing
- 23 • addressing
- 24 • allowing, allows
- 25 • applying . . . in combination
- 26 • arrangement
- 27 • aspect
- 28 • associated with
- authentication
- authorization information, authorized, not authorized
- budget control, budget

- 1 • can be
- 2 • capacity
- 3 • clearinghouse
- 4 • compares, comparison
- 5 • component assembly
- 6 • contain, contained, containing
- 7 • control (n.), controls (n.)
- 8 • controlling, control (v.)
- 9 • copied file
- 10 • copy, copied, copying
- 11 • copy control
- 12 • creating, creation
- 13 • data item
- 14 • derive, derives
- 15 • descriptive data structure
- 16 • designating
- 17 • device class
- 18 • digital signature, digitally signing
- 19 • entity, entity's control
- 20 • environment
- 21 • executable programming, executable
- 22 • execution space, execution space identifier
- 23 • generating
- 24 • govern, governed, governed item, governing
- 25 • halting
- 26 • host processing environment
- 27 • identifier, identify, identifying
- 28 • including
- 29 • information previously stored
- 30 • integrity programming
- 31 • key
- 32 • load module
- 33 • machine check programming
- 34 • metadata information
- 35 • opening secure containers
- 36 • operating environment, said operating environment
- 37 • organization, organization information, organize
- 38 • portion
- 39 • prevents
- 40 • processing environment

- protected processing environment
- protecting
- record
- required
- resource processed
- rule
- secure
- secure container, secure containers
- secure container governed item
- secure container rule
- secure database
- secure execution space
- secure memory, memory
- secure operating environment, said operating environment
- securely applying
- securely assembling
- securely processing
- securely receiving, securely receiving . . . a control
- security
- security level, level of security
- specific information, specified information
- tamper resistance
- tamper resistant barrier
- tamper resistant software
- tampering
- use
- validity
- virtual distribution environment

B. Claim Phrases and Clauses

‘193:1

- receiving a digital file including music
- a budget specifying the number of copies which can be made of said digital file
- controlling the copies made of said digital file
- determining whether said digital file may be copied and stored on a second device based on at least said copy control
- if said copy control allows at least a portion of said digital file to be copied and stored on a second device

copying at least a portion of said digital file

1 • transferring at least a portion of said digital file to a second device
2 • storing said digital file

3 '193:11

4 • receiving a digital file
5 • determining whether said digital file may be copied and stored on a second device based on
6 said first control
7 • identifying said second device
8 • whether said first control allows transfer of said copied file to said second device
9 • said determination based at least in part on the features present at the device
10 • if said first control allows at least a portion of said digital file to be copied and stored on a
11 second device
12 • copying at least a portion of said digital file
13 • transferring at least a portion of said digital file to a second device
14 • storing said digital file

15 '193:15

16 • receiving a digital file
17 • an authentication step comprising:
18 • accessing at least one identifier associated with a first device or with a user of said first device
19 • determining whether said identifier is associated with a device and/or user authorized to store
20 said digital file
21 • storing said digital file in a first secure memory of said first device, but only if said device
22 and/or user is so authorized, but not proceeding with said storing if said device and/or user is
23 not authorized
24 • storing information associated with said digital file in a secure database stored on said first
25 device, said information including at least one control
26 • determining whether said digital file may be copied and stored on a second device based on
27 said at least one control
28 • if said at least one control allows at least a portion of said digital file to be copied and stored
 on a second device,
 • copying at least a portion of said digital file
 • transferring at least a portion of said digital file to a second device
 • storing said digital file

29 '193:19

30 • receiving a digital file at a first device
31 • establishing communication between said first device and a clearinghouse located at a
32 location remote from said first device
33 • using said authorization information to gain access to or make at least one use of said first
34 digital file
35 • including using said key to decrypt at least a portion of said first digital file

- receiving a first control from said clearinghouse at said first device
- storing said first digital file in a memory of said first device
- using said first control to determine whether said first digital file may be copied and stored on a second device
- if said first control allows at least a portion of said first digital file to be copied and stored on a second device
- copying at least a portion of said first digital file
- transferring at least a portion of said first digital file to a second device including a memory and an audio and/or video output
- storing said first digital file portion

‘683:2

- 9 • user controls
- 10 • the first secure container having been received from a second apparatus
- 11 • an aspect of access to or use of
- 12 • the first secure container rule having been received from a third apparatus different from said second apparatus
- 13 • hardware or software used for receiving and opening secure containers
- 14 • said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers
- 15 • protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus
- 16 • hardware or software used for applying said first secure container rule and a second secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item contained in a secure container
- 17 • hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses.

‘721:1

- 20 • digitally signing a first load module with a first digital signature designating the first load
module for use by a first device class
- 21 • digitally signing a second load module with a second digital signature different from the first
digital signature, the second digital signature designating the second load module for use by a
second device class having at least one of tamper resistance and security level different from
the at least one of tamper resistance and security level of the first device class
- 22 • distributing the first load module for use by at least one device in the first device class
- 23 • distributing the second load module for use by at least one device in the second device class

‘721:34

26 • arrangement within the first tamper resistant barrier
27 • prevents the first secure execution space from executing the same executable accessed by a
28 second secure execution space having a second tamper resistant barrier with a second security
level different from the first security level

1

‘861:58

- 2 • creating a first secure container
- 3 • including or addressing . . . organization information . . . desired organization . . . and
- 4 metadata information at least in part specifying at least one step required or desired in creation
- 5 of said first secure container
- 6 • at least in part determine specific information required to be included in said first secure
- 7 container contents
- 8 • rule designed to control at least one aspect of access to or use of at least a portion of said first
- 9 secure container contents

10

‘891:1

- 11 • resource processed in a secure operating environment at a first appliance
- 12 • securely receiving a first entity's control at said first appliance
- 13 • securely receiving a second entity's control at said first appliance
- 14 • securely processing a data item at said first appliance, using at least one resource
- 15 • securely applying, at said first appliance through use of said at least one resource said first
- 16 entity's control and said second entity's control to govern use of said data item

17

‘900:155

- 18 • first host processing environment comprising
- 19 • said mass storage storing tamper resistant software
- 20 • designed to be loaded into said main memory and executed by said central processing unit
- 21 • said tamper resistant software comprising: . . . one or more storage locations storing said information
- 22 • derives information from one or more aspects of said host processing environment,
- 23 • one or more storage locations storing said information
- 24 • information previously stored in said one or more storage locations
- 25 • generates an indication based on the result of said comparison
- 26 • programming which takes one or more actions based on the state of said indication
- 27 • at least temporarily halting further processing

28

‘912:8

- 29 • identifying at least one aspect of an execution space
- 30 • required for use and/or execution of the load module
- 31 • said execution space identifier provides the capability for distinguishing between execution
- 32 spaces providing a higher level of security and execution spaces providing a lower level of
- 33 security
- 34 • checking said record for validity prior to performing said executing step

35

36

‘912:35

- received in a secure container
- said component assembly allowing access to or use of specified information
- said first component assembly specified by said first record

Dated: November 8, 2002

By: David J. Chelis

WILLIAM L. ANTHONY
ERIC L. WESENBERG
MARK R. WEINSTEIN
ORRICK HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400

STEVEN ALEXANDER
KRISTIN L. CLEVELAND
JAMES E. GINGER
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391

**Attorneys for Defendant
MICROSOFT CORPORATION**

Of Counsel:

T. Andrew Culbert, Esq.
One Microsoft Way
Building 8
Redmond, WA 98052-6399
Phone: 425-882-8080

1 **DECLARATION OF SERVICE BY E-MAIL AND FIRST CLASS MAIL**

2 I am more than eighteen years old and not a party to this action. My place of employment
3 and business address is 121 S.W. Salmon St., Suite 1600, Portland, OR 97204.

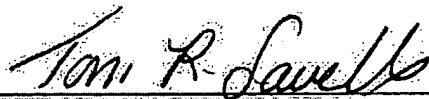
4 On November 8, 2002, I served on counsel for InterTrust Technologies Corporation:

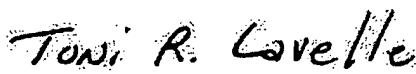
5 **MICROSOFT CORPORATION'S PATENT LOCAL RULE 4-1(a) STATEMENT** by e-
6 mail delivery and by placing true copies of these papers in envelopes addressed to:
7

| | |
|---|---|
| 8 Michael H. Page, Esq. 9 John W. Keker, Esq. 10 Jon B. Streeter, Esq. 11 KEKER & VAN NEST, LLP 12 710 Sansome Street 13 San Francisco, CA 94111 14 Phone: 415-391-5400 15 Fax: 415-397-7188 16 E-mail: mhp@kvn.com | 17 Stephen E. Taylor, Esq. 18 Taylor & Co. Law Offices 19 1050 Marina Village Parkway 20 Suite 101 21 Alameda, CA 94501 22 Phone: 510-865-9401 23 Fax: 510-865-9408 24 Email: staylor@tcolaw.com |
| 13 Steven H. Morrissey, Esq. 14 Finnegan Henderson Farabow 15 Garrett & Dunner 16 Stanford Research Park 17 700 Hansen Way 18 Palo Alto, CA 94304-1016 19 steven.morrissey@finnegan.com | |

20 and sealing each envelope, affixing adequate first-class postage and depositing it in the U.S. mail
21 at Portland, Oregon.

22 I declare under penalty of perjury that the foregoing is true and correct. Executed on
23 November 8, 2002, at Portland, Oregon.

24 
25 _____
26 (SIGNATURE)

27 
28 _____
29 (PRINT NAME)